



Medical Device Security: The Transition From Patient Privacy To Patient Safety

Scott Erven

Who I Am

Scott Erven



Associate Director – Medical Device & Healthcare Security



Security Researcher



***Over 15 Years Experience and 5 Years Direct Experience
Managing Security In Healthcare Systems***



Over 3 Years Researching Medical Device Security

@scotterven

Agenda

Why Research Medical Devices

Phase 1 Research: Device Vulnerabilities

Phase 2 Research: Internet Exposure

Phase 3 Research: Admin Access

Honeypot Research: Are Attacks A Reality?

Diagnosis

Problem Awareness

Treatment Plans



Why Research Medical Devices

Personal Impact

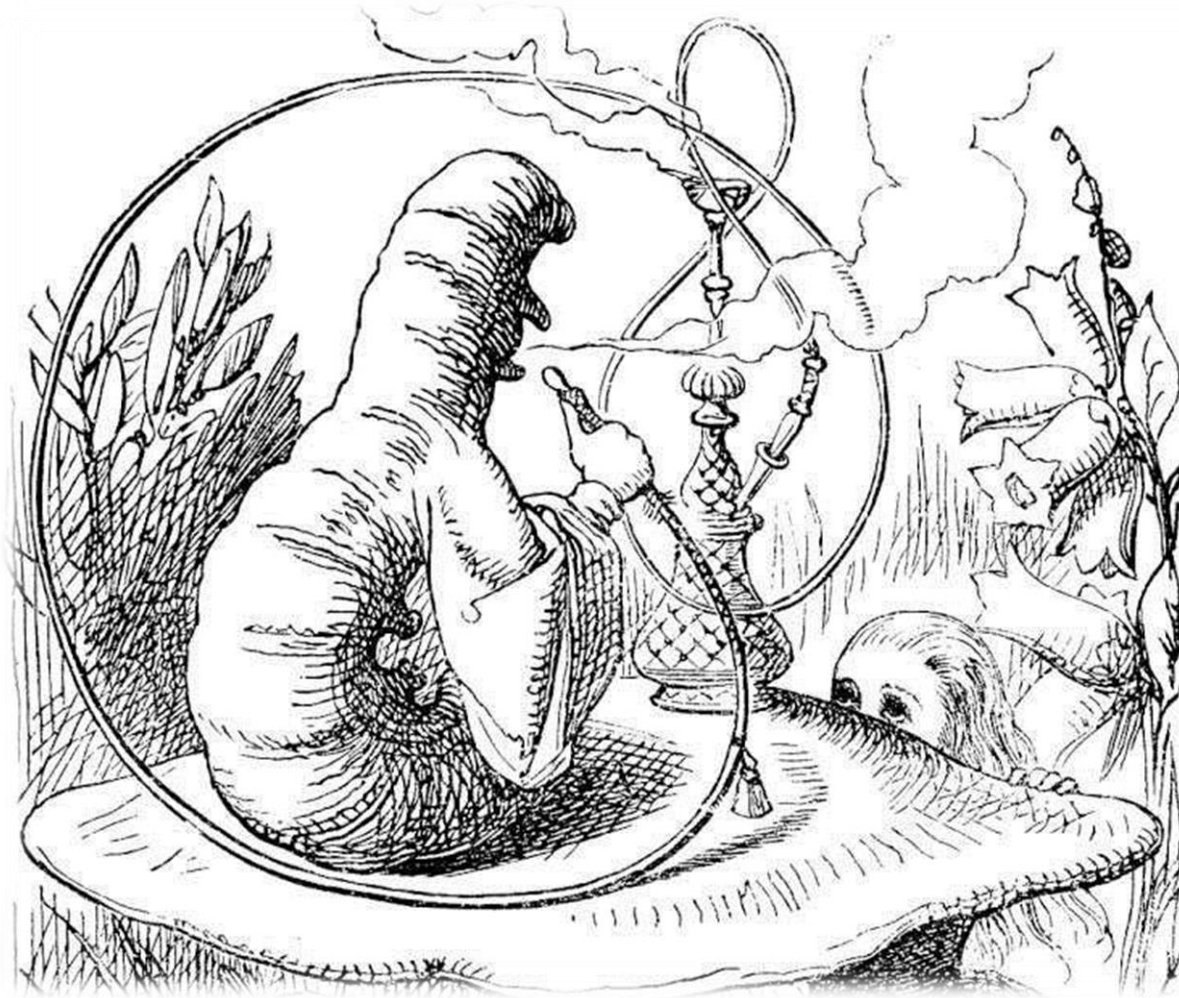
- Many of us rely on these devices daily.

- When we are at our most vulnerable, we will depend on these devices for life.

- Even at times when we aren't personally affected, people we care about may be.



Malicious Intent Is Not A Prerequisite To Patient Safety Issues



What We Are Doing

Medical Device Assessment

Discover patient safety issues

- Security-Focused Technical Assessment (not HIPAA)
- Research serves healthcare mission and values
- Equip defenders against accident and adversaries

Coordination & Notification

Alert affected parties

- Healthcare Providers
- Medical Device Manufacturers
- Government Agencies (FDA and ICS-CERT)

Public Awareness

Inoculate against future issues

- Security and Healthcare Conferences
- 1-on-1 with healthcare providers
- Educating FDA and Healthcare Providers



Phase 1 Research: Device Vulnerabilities

Phase 1 Research: Device Vulnerabilities

Weak default/hardcoded administrative credentials

- Treatment modification
- Cannot attribute action to individual

Known software vulnerabilities in existing and new devices

- Reliability and stability issues
- Increased deployment cost to preserve patient safety

Unencrypted data transmission and service authorization flaws

- Healthcare record privacy and integrity
- Treatment modification



Phase 2 Research: Internet Exposure

Shodan Search Initial Findings

Doing a search for anesthesia in Shodan and realized it was not an anesthesia workstation.

Located a public facing system with the Server Message Block (SMB) service open, and it was leaking intelligence about the healthcare organization's entire network including medical devices.



Initial Healthcare Organization Discovery



Very large US healthcare system consisting of over 12,000 employees and over 3,000 physicians. Including large cardiovascular and neuroscience institutions.

Exposed intelligence on over 68,000 systems and provided direct attack vector to the systems.

Exposed numerous connected third-party organizations and healthcare systems.

Did We Only Find One?

No. We found hundreds!!

Generic Search Examples:

shodan port:445 org:health*/clinic/hospital

health* - http://www.shodanhq.com/search?q=port:445+org:health*/clinic/hospital [.health](#) 148 hits

clinic - http://www.shodanhq.com/search?q=port:445+org:health*/clinic/hospital [clinic](#) 18 hits

hospital: http://www.shodanhq.com/search?q=port:445+org:health*/clinic/hospital [hospital](#) 119 hits

medical: http://www.shodanhq.com/search?q=port:445+org:health*/clinic/hospital [medical](#) 255 hits

Change the search term and many more come up. Potentially thousands if you include exposed third-party healthcare systems.

Let Me Paint The Picture

System with Lockout Exemption:

```
050580      Echo Vas OR 1 -  _ScreenLock_0_Exception
050581      _ScreenLock_0_Exception
050583      OR 1-  _ScreenLock_0_Exception
050585      Echo Vas OR 2 -  _ScreenLock_0_Exception
```

Impact:
System May Not Require Login

EMR:

```
EP03 EPIC Cogito Clarity RDBMs Server
EP04 EPIC Clarity Test Console
EP05 EPIC Business Objects test
EP06 EPIC Realy BCA Server 1
EP07 EPIC Hyperspace
EP08 EPIC Hyperspace Web Server 1
EP09 EPIC Hyperspace Web Server 2
EP10 EPIC Hyperspace Web Server 3
EP11 EPIC Web BLOB Server
EP12 EPIC Kuiper Server
EP13 EPIC EPS Server 1
EP14 EPIC EPS Server 2
EP15 EPIC Interconnect
EP16 EPIC Care Everywhere
EP17 EPIC Soap Proxy
EP18 EPIC System Pluse
EP19 EPIC Multipurpose SQL Server
EP20 EPIC - Citrix XenApp 6.5 License/Web
EP21 EPIC - Citrix XenApp 6.5 Application Server
EP22 EPIC - Citrix XenApp 6.5 Application Server/DC
EP23 EPIC My Chart
EP24 EPIC Care Link
EP25 EPIC File Service
```

Impact:
Electronic Medical Record Systems

Getting A Little Warmer!

Cardiology Systems:

060768 1 - Dr.
060911 D, Dr. C, Cath Lab Admin
061463 C - Cardiac Core Lab
063012 C - EP -
064320 Adrienne C - Cardiovascular Lab
065772 c **pacemaker**

069454 Go first floor Peds Nuclear Medicine

046142 Anesthesia OR

046774

046785 Me A

046798

046799 Da Fav

047271 **Anesthesia** Work Room

Impact:
Pacemaker Controller
Systems
Pediatric Nuclear Medicine
Anesthesia Systems

Summary Of Devices Inside Organization

Anesthesia Systems – 21

Cardiology Systems – 488

Infusion Systems – 133

MRI – 97

PACS Systems – 323

Nuclear Medicine Systems – 67



Potential Attacks - Physical

▶ *We know what type of systems and medical devices are inside the organization.*

▶ *We know the healthcare organization and location.*

▶ *We know the floor and office number.*

▶ *We know if it has a lockout exemption.*



Potential Attacks - Phishing

▶ *We know what type of systems and medical devices are inside the organization.*

▶ *We know the healthcare organization and employee names.*

▶ *We know the hostname of all these devices.*

▶ *We can create a custom payload to only target medical devices and systems with known vulnerabilities.*

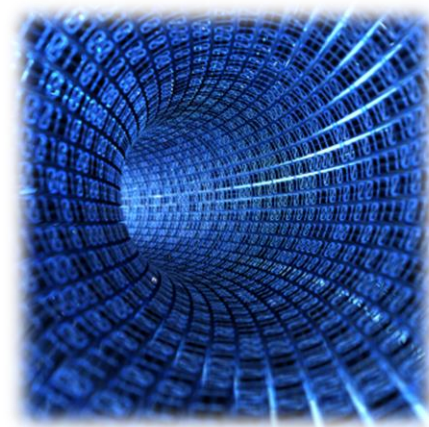


Potential Attacks - Pivot

▶ *We know the direct public Internet facing system is vulnerable to MS08-067 and is Windows XP.*

▶ *We know it is touching the backend networks because it is leaking all the systems it is connected to.*

▶ *We can create a custom payload to pivot to only targeted medical devices and systems with known vulnerabilities.*





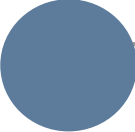
Phase 3 Research: Admin Access

Disclosure Timeline



NOTE: ALL INFORMATION DISCLOSED WAS PUBLICLY AVAILABLE ON GE HEALTHCARE'S WEBSITE.

Response



GE quickly responded to reports both from myself and ICS-CERT and outlined investigation plan for response.

After investigation GE responded that all credentials were default and not hard-coded.



CVE-2013-7404 CVSS = 10

GE Discovery NM750b – Nuclear Imaging

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Discovery	NM 750b	Nuclear Imaging	Telnet- Root	UserID = "insite" Password = "2getin"
GE	Discovery	NM 750b	Nuclear Imaging	FTP- Admin	UserID = "insite" Password = "2getin"

CVE-2011-5374

CVE-2011-5374 GE Discovery NM670/NM630 - Nuclear Imaging/CT

<i>Manufacturer</i>	<i>Model</i>	<i>Version</i>	<i>Type of Device</i>	<i>Type of Account</i>	<i>Login info</i>
GE	Discovery	NM670	Nuclear Imaging/CT	SU Account	UserID = "su" Password = "install"
GE	Discovery	NM670	Nuclear Imaging/CT	Service Account	UserID = "service" Password = "#bigguy1"
GE	Discovery	NM670	Nuclear Imaging/CT	Root Account	UserID = "root" Password = "install"
GE	Discovery	NM630	Nuclear Imaging	SU Account	UserID = "su" Password = "install"
GE	Discovery	NM630	Nuclear Imaging/CT	Service Account	UserID = "service" Password = "#bigguy1"
GE	Discovery	NM630	Nuclear Imaging/CT	Root Account	UserID = "root" Password = "install"

GE Login Credentials Word Cloud



So If They Are Indeed Default Are There Still Issues

- Documentation instructs in some cases to not change credentials and not allow password reset.
- Documentation instructs in some cases to not change password or your account will not be able to be supported.
- Documentation not updated with how to change default credentials and secure configuration guides are lacking.
- Support personal often rely on implementation documentation so these logins are heavily utilized in the healthcare industry.

Examples

3. When the *User Properties* screen appears, verify/change the following parameters and click **OK**.

- ◆ *User Must Change Password at Next Login*: Unchecked
- ◆ *User Cannot Change Password*: Checked
- ◆ *Password Never Expires*: Checked
- ◆ *Account Disabled*: Uncheck

Emergency Login

Click **Emergency Login** to launch the Emergency Login screen which does not require a ID or password that is filed on your Enterprise system.

3.3.2 Changing Passwords

You can change any of the account passwords with the following procedure.

Important

Do not change the InSite password. Remote access will be disabled for InSite support if the password is changed.

Examples

Table 3-8: Acquisition Passwords

Account User Name	Default Password
root	root.genie
service	service.
insite	insite.genieacq (Do not change this password!)
admin	admin.genie
reboot	reboot
shutdown	shutdown

Examples

Name	Password
MuseAdmin	Muse!Admin

NOTE: Tech Support will logon to the system with pcAnywhere using this user name and password.



Examples

Ask the remote station operator for your assigned username and **password**.

This resets the user's confirm password to **password**.

NOTE: To perform the following steps, you must generate X-ray radiation. Follow proper safety precautions with the X-ray system.

1. Turn on the digital system and login as service:
(user: **serviceapp** password: **orion**)
2. When the service application starts, select the **Calib** function on the *Main Menu*.
3. Select **System Manual Tab**.
4. Select **Overlay Tab**.
5. You should now see a white circle in the image display (you may want to minimize the calibration window). Activate fluoro radiation; center the II output phosphor within the outline circle by moving the camera/lens assembly position on the image intensifier (II).

Examples

WARNING



Adhere strictly to the procedures in this manual.

Some repair/replacement procedures require the removal of protective covers, exposing parts which may be heated to a high temperature, or potential pinch points.

To prevent burns or other injuries, read the safety/warning labels.

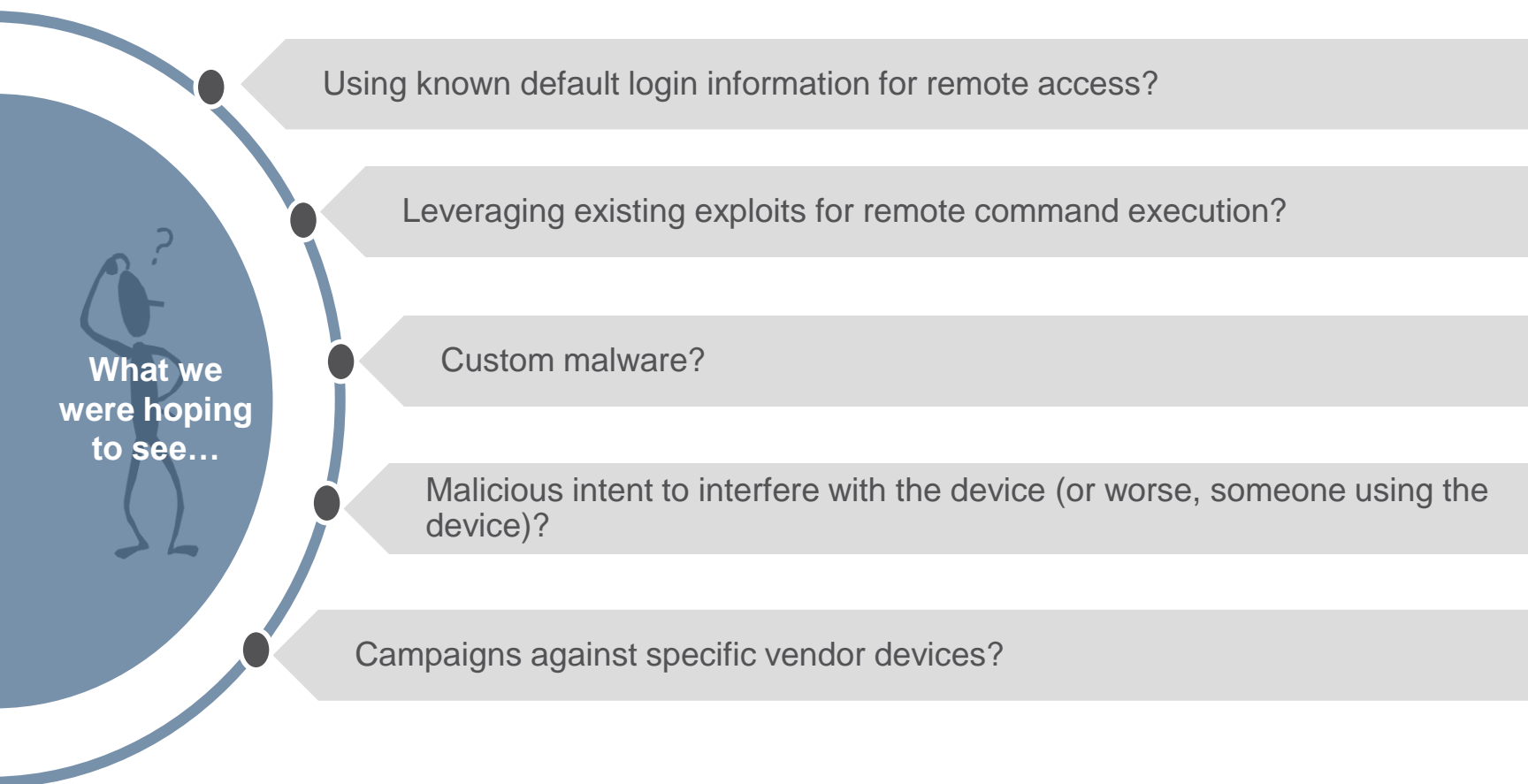


The editors and producers of this GE documentation site claim no responsibility for the accuracy, content, or availability of information contained on this site, or accessed or linked to through use of this site.



Honeypot Research: Are Attacks A Reality?

Real World Attacks



Real World Attacks – The Data

<i>Data</i>	
<i>Honeypots</i>	10
<i>Successful logins (SSH/Web):</i>	55,416
<i>Successful exploits (Majority is MS08-067)</i>	24
<i>Dropped malware samples</i>	299
<i>Top 3 Source Countries</i>	Netherlands, China, Korea
<i>HoneyCreds login</i>	8

HoneyCred logins are unique to the honeypot ssh/web service, someone did some research.

Real World Attacks – Conclusion

What did the attacker do once he got in?



Nothing

Did they realize they had root on a MRI machine?



Probably not

Are there owned medical devices calling back to a C2?



Yes

Do the C2 owners know what the information they are sitting on?



No

Real World Attacks – Conclusion

Have we seen evidence of intentional targeted attacks



Not yet

Are these devices being compromised due to unintentional attacks?



Absolutely



Diagnosis

Technical Properties



Exposed, vulnerable systems

- All software has flaws.
- Connectivity increases potential interactions.
- A software-driven, connected medical device is a **vulnerable, exposed** one.



Lack of patient safety alignment in medical device cyber security practices



Problem Awareness

Problem Awareness

Transition From Patient Privacy To Patient Safety

Health
Insurance
Portability
Accountability
Act



1 PATIENT
SAFETY
FIRST

Problem Awareness



1

***Medical devices** are **increasingly accessible** due to the nature of healthcare*

2

*HIPAA focuses on patient privacy, not **patient safety**.*

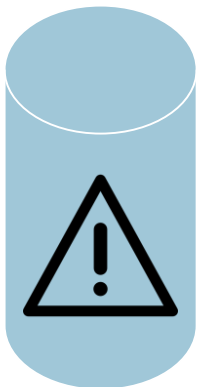
3

***FDA does not** validate **cyber safety** controls.*

4

***Malicious intent** is **not** a prerequisite for adverse patient outcomes.*

Isolation and Silos



Risk



Physicians



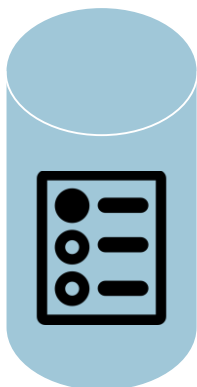
IT



Biomed



Legal



Compliance



Procurement

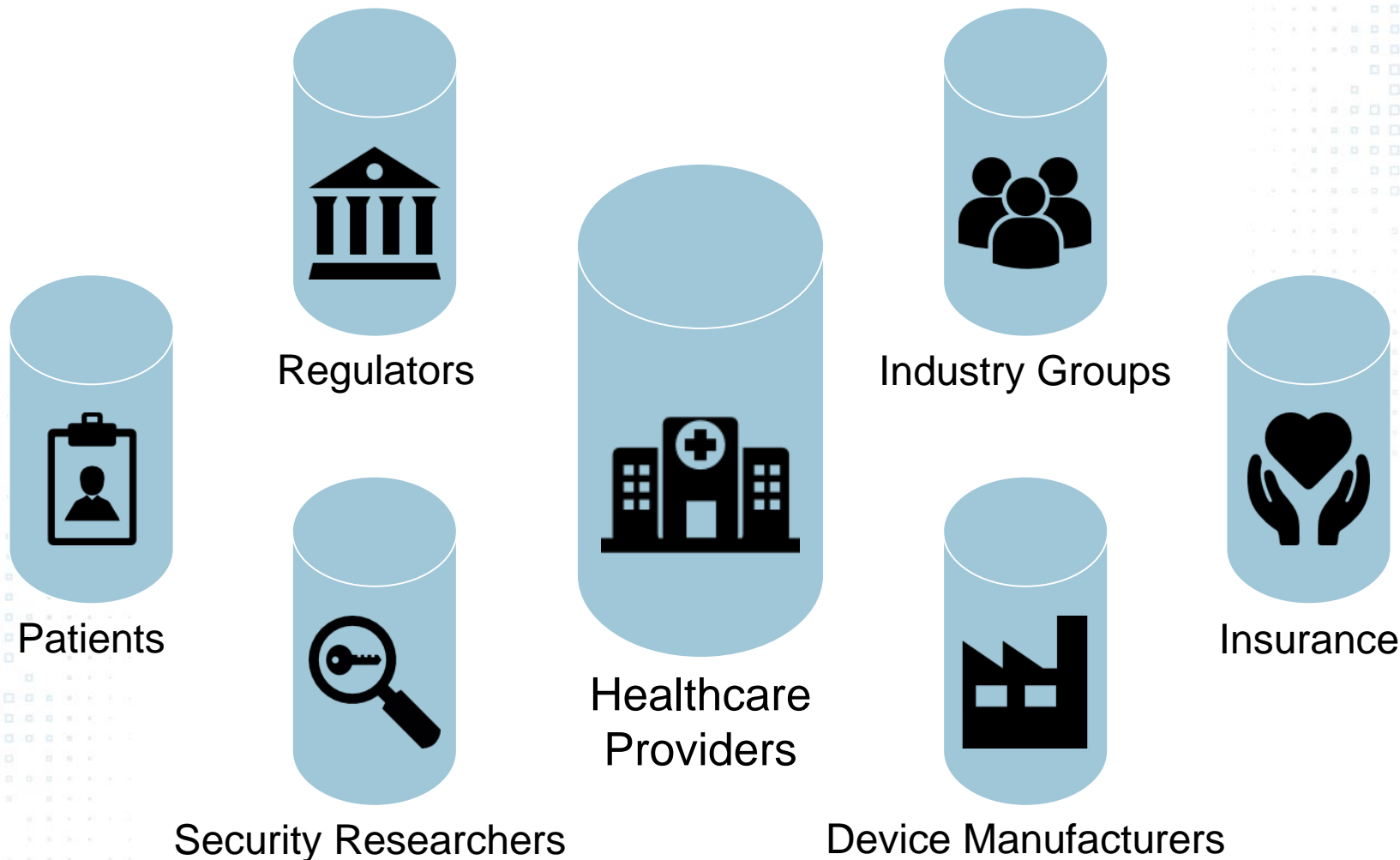


Administration



Board

Stakeholder Ecosystem





Treatment Plans

Treatment Plans

- Scan your biomedical device environment for default credentials and known security vulnerabilities.
- Report identified issues to manufacturer for remediation in your environment. Escalate to FDA if unresponsive.



Treatment Plans

*It falls to all of us. Patient safety is not a **spectator sport**.*



- **Stakeholders** must **understand** prerequisites
- **Multi-stakeholder** teams and conversations
- Engage with **willing allies** where domains of expertise overlap
- Incorporate **safety** into **existing processes**

Continue As-Is

Summary of Current State

- FDA receives “several hundred thousand” reports of patient safety issues per year related to medical devices
- Cyber safety investigations hampered by evidence capture capabilities.
- New devices are coming to market with long-known defects.
- Existing devices aren’t consistently maintained and updated.

A Better Way

Summary of Recommended Treatment

- Patient safety as the overriding objective
- Avoid failed practices and iteratively evolve better ones
- Engage internal and external stakeholders
- Safety into existing practices and governance

Projected Outcomes

- “Reliable medical devices to market without undue delay or cost.”
- Collaboration among willing allies on common terms
- Medical devices resilient against accidents and adversaries

Highlights From The Last 12 Months

- FDA Pre-Market Guidance and Workshop¹
- IEEE Workshop
- Embraced by healthcare community conferences
- Atlantic Council Cyber Wednesday²
- Vulnerability Disclosure Policies
- Vulnerability Disclosure Brainstorming and Education with FDA
- FDA Safety Communications BEFORE evidence of harm

¹<http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm>

²<http://www.atlanticcouncil.org/events/webcasts/cyber-risk-wednesday-the-healthcare-internet-of-things-rewards-and-risks>

Q&A

Scott Erven

Associate Director

Protiviti

Twitter: @scotterven

Email: scott.erven@protiviti.com